REMARKS

Claims 1-22 remain in the application, and reconsideration of this application is respectfully requested in view of the following arguments.

Allowable Claims

Applicants acknowledge that the Examiner has found that Claims 12-20 are allowable. Applicants further acknowledge that the Examiner has objected to Claims 5-7, and 10-11 as being dependent upon a rejected base claim but states that these claims would be allowable if rewritten in independent form, including all other limitations of the base claim and any intervening claims. Applicants submit that Claims 5-7 and 10-11 are allowable because the base claim, Claim 1, is allowable for all of the reasons argued below. Moreover, Applicants further submit that dependant Claims 2-4, 8-9, and 21-22 are allowable for all of the reasons argued below with respect to Claim 1.

Rejection of the Claims

The Examiner has rejected Claims 1-4, 8-9 and 21-22 under 35 U.S.C. § 103(a) as being unpatentable over Freeman (USPN 6,450,407) in view of Matyas, et al. (USPN 5,007,089). Applicants traverse these rejections.

To establish a *prima facie* case of obviousness under 35 U.S.C. §103 based upon the combined teaching of two or more references, three criteria must be met. First there must be some suggestion or motivation to combine the reference teachings. Second there must be a reasonable expectation of success, and finally, the references when combined must teach or suggest all of the claim limitations. *See* M.P.E.P. §2143. Applicants respectfully submit that the combined teachings of Freeman and Matyas, et al. do not render pending Claims 1-4, 8-9 and 21-22 obvious because the combined teachings fail to teach or suggest all of the claim limitations.

Specifically with respect to Claim 1, Applicants submit the both Freeman and Matyas, et al. fail to teach or suggest the limitations recited in Claim 1 of "*checking the identification code*

against a list stored locally at the card acceptance location, wherein the list is received from a second device" and "*if the identification code of the smart card is listed on the list, performing an action on the smart card.*" The Examiner conceded that Freeman fails to disclose these limitations but contends that Matyas, et al. discloses both limitations in col. 4, lines 5-50. Applicants respectfully disagree.

Applicants first submit that Matyas, et al. discloses a wholly different method from that claimed in the present invention. Specifically, Matyas, et al. teaches a method for "updating of control vector checking code" in a cryptographic device, such as a smart card. (Col. 2, lines 55-57; *see also* col. 3, lines 36-39; and col. 8, lines 1-6). In accordance with Matyas, et al., a cryptographic facility residing on the cryptographic device (e.g., a smartcard) receives cryptographic requests from a set of applications programs also residing on the smartcard. The cryptographic facility either accepts or rejects these requests based upon the outcome of a validity check performed by a control vector checking unit also residing on the smartcard. The control vector checking unit uses a sequence of rules or instructions called CV (control vector) checking code to perform these validity tests. The method disclosed in Matyas, et al. is one for dynamically and securely modifying or enhancing the CV checking code used by the CV checking unit of the smartcard. (*See* Col. 3, lines 39-53).

In order for the smartcard to modify its CV checking code, it retrieves the code update from a CV checking code repository that may be located on the smartcard in one embodiment or at a remote location (e.g., a different cryptographic device from the smartcard) in another embodiment. (*See* Figs. 2 and 3). It then performs a cryptographic authentication process on the retrieved code to verify that the downloaded code was received with integrity. If the authentication of the downloaded CV code is successful, then the smartcard may implement the code. Otherwise the code is discarded and an authentication error regarding the downloaded CV code may be reported. (*See* col. 4, lines 5-25 and col. 8, lines 18-35 and 41-46).

Regarding Claim 1, the Examiner asserts that at col. 4, lines 5-50 of Matyas, et al., it discloses checking the smartcard's ID code against a list stored locally at the card acceptance location, wherein the list is received from a second device. Applicants respectfully disagree with the Examiner. The language that the Examiner quotes describes Fig. 2 of Matyas, et al. Fig. 2 illustrates 2 devices, a first cryptographic device 100 (e.g., a smartcard (*See* Fig. 10)) and an optional second cryptographic device 200 (e.g. a smartcard reader or card acceptance location

(*See* Fig. 10)). The card acceptance location 200 is illustrated only as having a repository for CV checking code that may be used to update the CV code in the smartcard. There is no illustration in Fig. 2 or disclosure in the accompanying language cited by the Examiner of the card acceptance location 200 storing a list against which an identification code of the smartcard 100 might be checked, as claimed in Claim 1 and included by dependency in Claims 2-4, 8-9 and 21-22. The only list that is taught in Matyas, et al. is a list of modification detection code (MDC) values that, in one embodiment, may be stored in the *smartcard* 100 and used for verifying the integrity of the downloaded CV checking code. (*See* col. 4, lines 50-68). Moreover, the language of Matyas, et al. even fails to mention an identification code for the smartcard 100.

Applicants further submit that there is no *second device* taught in Matyas, et al. from which the card acceptance location 200 could receive a list, as claimed in Claim 1 and included by dependency in Claims 2-4, 8-9 and 21-22. Matyas, et al. only teaches the smartcard 100 and optionally the smartcard reader 200 (where the CV checking code repository is not located locally on the smartcard). There is no other device mentioned that could be read as a *second device* as claimed in Claim 1 and included by dependency in Claims 2-4, 8-9 and 21-22.

The Examiner further asserts that col. 4, lines 5-50 of Matyas, et al. teaches that if the ID code of the smartcard is listed on the list, performing an action on the smartcard. Applicants again respectfully disagree. Applicants submit that in accordance with the language of Matyas, et al. in the system embodiment wherein a smartcard acceptance location 200 is used, there is no action performed by the smartcard acceptance location on the smartcard, as claimed in Claim 1 and included by dependency in Claims 2-4, 8-9 and 21-22. The smartcard acceptance location is simply used to send updated CV checking code to the smartcard 100 as requested by the smartcard. (*See* Figs. 2 and 10; col. 4, lines 2-25 and col. 8, lines 18-28).

For all of the above reasons, either Freeman or Matyas, et al. alone or in combination do not render Claim 1 obvious. Therefore, Applicants submit that Claim 1 is in a condition for allowance. Moreover, Claims 1-11, 21 and 22 that depend either directly or indirectly from Claim 1 are likewise in a condition for allowance.

In further regard to Claim 2, the Examiner concedes that Freeman does not disclose the limitation recited in Claim 2 of "*wherein the action is selected from a group consisting of disabling the smart card, enabling the smart card.*" However, the Examiner contends that Matyas, et al discloses this limitation at col. 4, line 50 through col. 5, line 20. Applicants

disagree. In accordance with Claim 2 of the present invention, the disabling or enabling of the smart card is performed "*if the identification code of the smart card is listed on the list.*" As argued earlier, neither Freeman nor Matyas, et al. discloses a list stored locally at a card acceptance location against which an identification code can be checked. Moreover, the language in Matyas, et al. cited by the Examiner does not teach the smart card 100 being enabled and disabled as claimed in Claim 2, but teaches either that the downloaded CV checking code will be used by the smartcard 100 or discarded depending upon the results of the authentication check by the smartcard of the code. Therefore, for these additional reasons, Applicants submit that Claim 2 is in a condition for allowance.

In further regard to Claims 3-4 and Claims 21-22, the Examiner states that Matyas, et al. discloses in Col. 4, line 50 to col. 5, line 20 every limitation recited in these claims. Applicants disagree. Upon a close review of the language in Matyas, et al. cited by the Examiner, Applicants were unable to find any references to the smart card having status data, as recited in Claims 3 and 4. Likewise, in regard to Claims 21 and 22, Matyas, et al. fails to disclose the smart card having a status bit. Therefore, for these additional reasons, Applicants submit that Claims 3-4 and 21-22 are in a condition for allowance.

The Applicants note the art cited, but not relied upon by the Examiner.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicants have argued herein that such amendment was made to distinguish over a particular reference or combination of references.

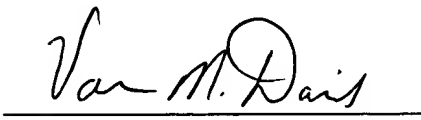
The Applicants believe that the subject application, as amended, is in condition for allowance. Such action is earnestly solicited by the Applicants.

In the event that the Examiner deems the present application non-allowable, it is requested that the Examiner telephone the Applicants' attorney or agent at the number indicated below so that the prosecution of the present case may be advanced by the clarification of any continuing rejection.

Accordingly, this application is believed to be in proper form for allowance and an early notice of allowance is respectfully requested.

Please charge any fees associated herewith, including extension of time fees, to Deposit Account No. 502117.

Respectfully submitted,

By: 

Valerie M. Davis
Attorney of Record
Reg. No.: 50,203
Telephone:(847) 576-6733
Fax No.: (847) 576-0721

SEND CORRESPONDENCE TO:

Motorola, Inc.
Law Department

Customer Number: 22917